



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/924,585	08/09/2001	Yasutaka Sato	062800-0103	2998

22428 7590 02/22/2005

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/924,585

Applicant(s)

SATO, YASUTAKA

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 08092001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Specification

Claim Objections

The examiner assumes that the applicant is referring to the process where an output unit accepts data grouped in bytes and frames and processes the data for continuous serial binary output.

Appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2137

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5 Claims 1-3 and 17-19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The applicant claims that the determination unit looks for a "predetermined continuous pattern" before it begins to add or subtract values as prescribed by the calculation unit. While the applicant's summary of the invention repeats the exact claim, the description of the invention discloses that the
10 determination unit looks for a predetermined byte code or value.

 While the examiner understands how the determination unit can look for a predetermined pattern, the examiner is unclear how the determination unit can look for a predetermined *continuous* pattern. If the pattern that the unit seeks is continuous or extending to infinite, it is unclear how the unit can possibly know when it has found the continuous pattern. The examiner suggests that the word continuous be
15 removed from the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 102

 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

20 A person shall be entitled to a patent unless –

 (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

25

 Claims 1-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Karppanen, U.S. Patent No. 5,987,137.

 As per claim 1, the applicant describes a data protection processing device which comprises the
30 following limitations which are met by Karppanen:

Art Unit: 2137

a) a determination unit which reads continuous digital data in sequence and determines whether or not the read digital data forms numerical values having a predetermined continuous pattern (Col 9, lines 53-62);

5 b) a calculation unit which adds predetermined calculation values to or subtracts predetermined calculation values from either all of or a portion of a predetermined number of items of digital data that are continuous after digital data that is determined as a result of the determination by the determination unit to form numerical values having the predetermined continuous pattern (Col 7, lines 16-19);

10 Karppanen discloses a communication system where a mobile user can connect with a network (see Fig 4b). The data that is transmitted between the two entities is secure because a secret key adds values to blocks of data so that it is sent in an enciphered form. The corresponding secret key on the receiving end uses the key to add values to the enciphered text to recover the plain text message.

15 Regarding part a), Karppanen discloses two entities exchanging clear text messages in a synchronized fashion. The system switches to an encipher/decipher mode when a "start cipher" command is sent on the network side to the mobile station. Since the "start cipher" command is a command which is transmitted to the mobile station, it is sent in binary which has a numerical value. The applicant should also note that Karppanen further discloses the use of a bit in a frame to direct the system as to whether or not to encipher or decipher the data in the frame even if the "start cipher" command has already been sent (Col 6, lines 25-27). Though a determination unit is not explicitly expressed, it is inherent in Karppanen that there is a mechanism for determining whether or not to encipher data and this
20 unit or mechanism corresponds to the determination unit of the applicant.

Regarding part b), the calculation unit enciphers data once a "start cipher" command has been recognized. The calculation unit is represented by the bitwise binary addition block of Fig 4b. Block 1, which is a function of the key, is combined with the plain text in a bitwise binary addition and cipher text is output for transmission as a result.

Art Unit: 2137

As per claims 2,5,8,11,15,18,21,24,27,30, and 33, the applicant describes the data protection processing device of claims 1,4,7,10,13,17,20,23,26,29, and 32, which are anticipated by Karppanen (see above), with the following additional limitation:

5 Wherein the calculation unit sequentially adds or subtracts calculation values of predetermined data patterns or byte patterns to or from digital data or byte data that is the object of the addition or subtraction (Col 7, lines 16-19);

The applicant can see from Fig 4b that the enciphering process is a sequential process where plain text is inputted with block 1 into a bit wise binary addition unit and enciphered or encrypted text is output for transmission.

10 The applicant should also note that since "an output bit string (Block 1) is summed to the sub-block (plain text in)" (Col 7, lines 16-17), Block 1 is in a predetermined data pattern or byte pattern to match that of the plain text in (Col 6, lines 25-30).

15 As per claims 3,6,9,12,19,22,25,28,31, and 34, the applicant describes the data protection processing device according to claim 1, which is anticipated by Karppanen (see above), with the following additional limitations which are also anticipated by Karppanen:

- a) a memory which stores information relating to the predetermined numerical values or the predetermined byte code, information relating to the predetermined number of items, and information relating to the predetermined calculation values (Col 9, lines 53-62; Col 9, lines 20-25);
- 20 b) an information altering unit which alters at least one from among the information relating to the predetermined numerical values or the predetermined byte code, the information relating to the predetermined number of items, and the information relating to the predetermined calculation values that are stored in the memory (Fig 4b; Col 9, lines 11-19);

25 Regarding part a), since the network and the mobile station both have a way of recognizing a "start cipher" command (Col 9, lines 53-62), both of them must have information relating to the "start cipher" command, or byte code, stored in memory. This is also information related to the predetermined number of items because the number of frames that the enciphering key operates on is a function of

Art Unit: 2137

when the "start cipher" command has executed. Lastly, information relating to the predetermined calculation values is information about the ciphering key, which is stored in memory and which generates the addition of values to the plain text.

Regarding part b), the information altering unit is described by the applicant as a unit which stores
5 and provides data, such as adding conditions, adding range, and protection key values for the calculation unit. In regards to Fig 4b and the lines referenced above, the information altering unit corresponds to the unit which stores and matches the count synchronization data and the key data which are processed to produce output Block1 for the calculation unit.

Regarding claim 16, the use of synchronization data is disclosed (Col 3, lines 51-53) as
10 corresponding to the Count data.

As per claims 4 and 20, the applicant describes the limitations of claim 1, which is met by Karppanen (see above), and the following additional limitations which are also met by Karppanen:

a) a holding unit which converts binary data input serially into byte data and temporarily holds the
15 byte data (Col 7, lines 29-30);

d) an output unit which converts byte data calculated by the calculation unit into binary data and serially outputs the binary data (Fig 4b);

Regarding part a), data is transmitted in serial binary but received and processed in frames which can be six to eight bits (Col 7, lines 29-30). Since eight bits is a byte, a frame is described as having the
20 length of a byte. The frames are what are processed throughout the enciphering process. Furthermore, data is packaged for transmission and reception in frames (Col 2, lines 8-11) but sent as a serial representation of binary data because only the transmitter and receiver can interpret the frames, not the transmission medium, in which the data looks merely like a continuous stream of data.

The applicant should also note that determination of when to start an enciphering/deciphering
25 sequence is done once a predetermined byte code, or "start cipher" command is received. Thus, the process by which data is communicated between the two entities is initially receiving clear text, receiving a "start cipher" command, and then beginning the enciphering/deciphering process. The process is an

Art Unit: 2137

exact parallel of the applicant's process where a number or flag commences the enciphering/deciphering process.

Though a holding unit is not explicitly described, it is inherent in the art that there is a mechanism which holds the data from the time it is received as serial binary data to be put into frames to the time it is
5 processed in the calculation unit as a frame sequence.

As per claims 7,13, and 26, the claims present the data protection processing device of claim 1 with a second determination and calculation unit. Fig 4b discloses a system with two calculation units, one on the network side for enciphering a message and one on the mobile station side for deciphering a
10 message. The use of two determination units is disclosed in Col 7, lines 16-24 because both the network side and the mobile station side have to be able to determine when to begin the enciphering/deciphering phase. This satisfies claims 13 and 26.

Claim 7 discloses the use of both the first and second determination and calculation units on the same device. Karppanen's system takes place in a bidirectional environment where both the network and
15 the mobile station are equipped with transmission/reception calculation units. As described in Col 9, lines 53-62, the network side commences the enciphering/deciphering of information once a determination has been made that a received "start cipher" message has been received and deciphered (Col 9, lines 53-62). A deciphering unit is separate from the enciphering unit because the deciphering unit combines enciphered text with a key (block 1) to form plain text while an enciphering unit combines plain text with a
20 key (block 1) to form enciphered text.

The use of the network side having an enciphering calculation unit is illustrated in Fig 4b. Furthermore, it is inherent in the art that there is a determination unit which decides, based on whether the "start cipher" message has been received, whether or not to pass the information to be transmitted through the enciphering method.

Art Unit: 2137

As per claim 10, the applicant describes a modem device with the limitations of claim 7, which are anticipated by Karppanen (see above), and the following additional limitations which are also anticipated by Karppanen:

a) a data compression unit which performs data compression processing on a digital data to be transmitted based on a normalized data compression standard (Col 3, lines 1-6);

f) a data decompression unit which converts byte data subtracted or added in the second calculation unit into digital data and performs data decompression processing on the converted digital data based on the data decompression standard (Col 3, lines 1-6);

The use of a modem, or "data transmission link to a mobile station" (Col 3, lines 20-21), and the internet (Col 3, line 18) is disclosed by Karppanen. The use of compressing data to be enciphered is disclosed (Col 3, lines 1-6), as the SNDC layer is where compression and enciphering take place. Since deciphering also takes place at the SNDC layer, it is inherent that decompression takes place here as well when a compressed, enciphered message is sent for decompression and deciphering.

As per claim 14, the applicant describes the data communication system according to claim 13, which is met by Karppanen (see above), with the following additional limitation which is also met by Karppanen:

Wherein the data transmitting device and data receiving device are connected to each other via a network such as the Internet (Col 3, lines 15-21).

As per claim 23, the applicant describes the limitations of claim 4, which is met by Karppanen (see above), with the following additional limitations which are also met by Karppanen:

b) a data extraction processing step of extracting a portion of the byte data forming the predetermined data frames held in the holding step to serve as data for processing (Col 6, lines 25-27);

e) a data frame reconstruction processing step of reconstructing the predetermined data frames using byte data calculated in the calculation processing step (Col 5, lines 14-17; Col 2, lines 8-11);

Art Unit: 2137

Data within the network and mobile station systems is processed in frames (Col 2, lines 8-11). Regarding part b), once the data is serially received and framed, extra bits in the frame such as bits which tell the frame whether or not the data is to be ciphered or not ciphered are read (Col 10, lines 16-22). The remaining data is extracted and processed with the ciphering key bit by bit in the calculation unit (Col 6, lines 25-27) given that the determination unit has determined that the data is not the "start cipher" command and the "start cipher" command has already been sent to set up the mutual exchange of enciphered or deciphered information.

As per claim 29, the claim includes limitations a) through d) which are met by the rejection for claim 4. Having a parallel receiving unit which has limitations e) through h) is met by the rejection for claim 7.

As per claim 32, the claim includes limitations a) through f) which are met by the rejection for claim 23. Having a parallel receiving unit which has limitations g) through l) is met by the rejection for claim 7.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
5 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER